21

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-132253
(43)Date of publication of application : 09.05.2003

(51)Int.Cl. G06F 17/60
H04L 9/08
H04L 9/32

(21)Application number : 2001-323624
(22)Date of filing : 22.10.2001

(71)Applicant : KDDI CORP
COMMUNICATION RESEARCH LABORATORY
(72)Inventor : KIYOMOTO SHINSAKU
TANAKA TOSHIAKI
NAKAO KOJI
FUJISE MASAYUKI
KOJIMA FUMIHIDE
SATO KATSUYOSHI

(54) SERVICE RESERVATION AND PROVIDING METHOD FOR MUTUAL AUTHENTICATION BY USE OF TICKET, PROGRAM THEREFOR, AND STORAGE MEDIUM WITH PROGRAM STORED THEREIN

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a mutual authentication processing method and program allowing even a terminal with low processing power to have sufficient authentication ability without using a public key cryptosystem for each of reservation stage and providing stage of a service in electronic commerce, and a storage medium with the program stored therein.
SOLUTION: In the service reservation stage, mutual authentication is performed (S31-S3B), and a server transmits reservation ticket information to a terminal (S3E) and also stores the reservation ticket information. In the service providing stage, both the server and the terminal generate a common key KCS based on the reservation ticket information (S41-S47) to perform the authentication of the reservation ticket information with the server by use of the common key KCS (S48-S4B), and the

server transmits service information to the terminal (S4D).

LEGAL STATUS

[Date of request for examination]	19.04.2004
[Date of sending the examiner's decision of rejection]	
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]	
[Date of final disposal for application]	
[Patent number]	3940283
[Date of registration]	06.04.2007
[Number of appeal against examiner's decision of rejection]	
[Date of requesting appeal against examiner's decision of rejection]	
[Date of extinction of right]	

CLAIMS

[Claim(s)]

[Claim 1] the service reservation authentication phase (S31-S3B) which attests a server and a terminal mutually as a service reservation phase, and this server -- reservation ticket information -- said terminal -- transmitting (S3E) -- It has the reservation ticket transmitting phase of memorizing this reservation ticket information. As a service provision phase The common key generation phase to which both a server and a terminal generate the common key KCS based on said reservation ticket information (S41-S47), The service provision authentication phase which attests said server and said reservation ticket information using this common key KCS (S48-S4B), The service reservation and the offer approach which said server attests mutually using the ticket characterized by having the service information transmitting phase (S4D) of transmitting said service information to said terminal.

[Claim 2] The approach according to claim 1 which said server of said service reservation phase and said server of said service provision phase are with the 1st server different, respectively and the 2nd server different, respectively, and is characterized by having the phase where said 1st server transmits said reservation ticket information to said 2nd server.

[Claim 3] The approach according to claim 1 or 2 that said terminal of said service reservation phase and said terminal of said service provision phase are with the 1st terminal different, respectively and the 2nd terminal different, respectively, and said 1st terminal is characterized by having the phase of transmitting said reservation ticket information to said 2nd terminal.
[Claim 4] Said common key generation phase of said service provision phase is an approach given in any 1 term of claims 1-3 characterized by what (S46, S47) said common key KCS is generated for based on the hash value computed from said reservation ticket information.
[Claim 5] Said common key generation phase of said service provision phase The phase where said terminal generates the 3rd random number (R) itself (S42), and transmits this 3rd random number (R) and said reservation ticket information identifier (t-ID) to said server (S43), The phase where said terminal generates said common key based on said hash value, and said 3rd random number (R) and said reservation ticket information identifier (t-ID) (S47), The approach according to claim 4 characterized by said server having the phase (S46) which generates said common key based on said hash value, and said 3rd random number (R) and said reservation ticket information identifier (t-ID).
[Claim 6] Said service provision authentication phase of said service provision phase The phase where said server transmits said 3rd random number (R) enciphered using said common key to said terminal (S48), The phase where said terminal decrypts said 3rd enciphered random number (R), compares this 3rd decrypted random number (R) with said 3rd random number (R) generated itself, and attests said server (S49), The phase of transmitting said reservation ticket information enciphered to said attested server using said common key to said server (S4A), The approach according to claim 5 characterized by having the phase (S4B) which said server decrypts said enciphered reservation ticket information, compares this decrypted reservation ticket information with said reservation ticket information which said server published, and attests said reservation ticket information.
[Claim 7] said service provision phase -- said service information transmitting phase (S4D) -- then, an approach given in any 1 term of claims 1-6 to which said terminal is further characterized by having the phase (S4G) of canceling said reservation ticket information, and the phase (S4F) where said server cancels said reservation ticket information.
[Claim 8] The phase where said terminal transmits a terminal side identifier (IDA) to said server, It has further the terminal registration phase (S30) which consists of a phase where said server transmits said terminal side identifier (IDA) which received, and the key (MA) based on the private key (P) of the server concerned to said terminal. Said service reservation authentication phase of said service reservation phase The phase where said terminal generates the 1st random number (R) itself (S31), and transmits this 1st random number (R) and a terminal side identifier (IDA) to

said server (S32), The phase where said terminal generates the prior common key MAS based on said key (MA), said terminal side identifier (IDA), and said 1st random number (R) (S34), The phase (S33) where said server generates the prior common key MAS using said function (fMA) based on said terminal side identifier (IDA) and the key (MA) based on the private key (P) of the server concerned and said terminal side identifier (IDA), and said 1st random number (R), and said server The phase which generates the 2nd random number (R') itself (S35), enciphers said the 1st random number (R) and this 2nd random number (R') with said prior common key MAS, and is transmitted to said terminal (S36), The phase where said server generates the common key KAS based on said terminal side identifier (IDA) and said 2nd random number (R') (S37), Said terminal decrypts said the 1st random number (R) and said 2nd random number (R') using said prior common key MAS. The phase which attests said 1st server and generates the common key KAS based on said terminal side identifier (IDA) and said 2nd decrypted random number (R') when this 1st decrypted random number (R) is in agreement (S38), The phase which said terminal enciphers said the 2nd random number (R') and user certificate using said common key KAS, and transmits to said server (S39), Said server decrypts said the 2nd random number (R') and said reservation ticket information using said common key KAS. An approach given in any 1 term of claims 1-7 characterized by having the phase (S3A) which attests said terminal when this 2nd decrypted random number (R') is in agreement.

[Claim 9] It is an approach given in any 1 term of claims 1-8 characterized by for said server giving the signature of said server to said reservation ticket information about the reservation ticket transmitting phase of said service reservation phase, and said terminal giving the signature based on said terminal side identifier to said received reservation ticket information.

[Claim 10] A service reservation authentication means by which a terminal attests a server about a service reservation means (S38), A means (S3E) to receive reservation ticket information from this server, and a common key generation means to generate the common key KCS about a service provision phase based on said reservation ticket information (S47), The service reservation and the distribution program by the side of the terminal characterized by operating a computer as a service provision authentication means (S49) to attest said server using this common key KCS, a service reservation authentication means (S3A) by which a server attests a terminal about a service reservation means, and reservation ticket information -- said terminal -- transmitting (S3E) -- A reservation ticket transmitting means to memorize this reservation ticket information, and a common key generation means to generate the common key KCS about a service provision phase based on said reservation ticket information (S46), The service reservation and the distribution program by the side of the server characterized by operating a computer as a service provision authentication means (S4B) to attest said reservation ticket information using this common key KCS, and a service information transmitting means (S4D) to

transmit said service information to said terminal.
[Claim 11] The record medium which recorded the program according to claim 10.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention] This invention relates to the record medium which recorded the approach, the program, and this program of the mutual recognition processing produced in each of the reservation phase of service, and an offer phase in electronic commerce.
[0002]
[Description of the Prior Art] In recent years, the technique which downloads at a going-out place by development of communication technology with the mounted terminal in the terminal and ITS (altitude transportation system) which carry mass multimedia contents etc., and is perused is beginning to be examined. With such service, a user is the terminal which performs a certain service reservation at a domestic terminal, and is carried at a going-out place, and takes the gestalt of using the reserved service. that time -- a user -- becoming completely -- etc. -- in order to prevent unjust use, it is necessary to attest a user appropriately Conventionally, same authentication processing was performed in each scene. Especially, the public-key-encryption-ized method was adopted for authentication processing.
[0003] Drawing 1 is the target system configuration [this invention] Fig. According to drawing 1 , the service reception server 12 which reserves service, the service provision server 11 which offers service, and the management server 10 which manages them are expressed. As for these, interconnecting through the Internet is desirable. Moreover, a user's terminal 14 can access the service reception server 12, and can reserve specific service after fixed authentication processing. Moreover, it can access to the service provision server 11, and offer of specific service can be received not only from the reserved terminal 14 but from other personal digital assistants 13 after fixed authentication processing.
[0004] Drawing 2 is the conventional authentication sequence diagram. First, Server A transmits a request to Server B (S21). By the request, the public key PA and certificate of Server A are transmitted to Server B. Server B checks a certificate and generates a random number (R) (S22). Next, Server B transmits the random number (R) enciphered with the public key PA of Server A, the identifier (IDB) of Server B, and the public key PB and certificate of Server B (S23). The server A which received these checks a certificate (S24), and decrypts the enciphered random number (R) and

the identifier (IDB) of Server B. Furthermore, Server A generates random-number R' and transmits the identifier (IDA) of the random number (R, R') enciphered with the public key PB of Server B, and Server A to Server B (S25). Thereby, Server B decrypts the enciphered random number (R, R'), and when the random number (R) is in agreement, it attests Server A (S26). Thereby, Server A and Server B generate the common key KAB, respectively (S27, S28). Next, Server B transmits the random number (R') enciphered with the common key KAB to Server A (S29). Thereby, Server A decrypts the enciphered random number (R'), and when the random number (R') is in agreement, it attests Server B (S2A, S2B).

[0005]

[Problem(s) to be Solved by the Invention] However, always using a public-key-encryption-ized method, in order to attest a user enlarges the load of authentication processing. In order to carry out with a personal digital assistant like PDA with a comparatively low throughput unlike an installed terminal equipment like a personal computer, this problem becomes remarkable and that processing takes very long time amount to it. Consequently, the convenience of service may fall.

[0006] Then, this invention aims at offering the record medium which recorded the approach, the program, and this program of the mutual recognition processing which can have authentication capacity sufficient also at the low terminal of a throughput about each of the reservation phase of the service in electronic commerce, and an offer phase, without using a public key cryptosystem.

[0007]

[Means for Solving the Problem] According to the service reservation and the offer approach of attesting mutually using the ticket of this invention the service reservation authentication phase (S31-S3B) which attests a server and a terminal mutually as a service reservation phase, and this server -- reservation ticket information -- a terminal -- transmitting (S3E) -- It has the reservation ticket transmitting phase of memorizing this reservation ticket information. As a service provision phase The common key generation phase to which both a server and a terminal generate the common key KCS based on reservation ticket information (S41-S47), It has the service provision authentication phase (S48-S4B) which attests a server and reservation ticket information using this common key KCS, and the service information transmitting phase (S4D) where a server transmits service information to a terminal. That is, the description of this invention can publish reservation ticket information, after performing authentication suitable in the case of the first authentication, and it can mitigate the load for authentication processing by attesting using reservation ticket information about subsequent authentication processing.

[0008] According to other operation gestalten of the approach of this invention, the server of a service reservation phase and the server of a service provision phase are with the 1st server different, respectively and the 2nd server different, respectively,

and it is also desirable to have the phase where the 1st server transmits reservation ticket information to the 2nd server.

[0009] According to other operation gestalten of the approach of this invention, the terminal of a service reservation phase and the terminal of a service provision phase are with the 1st terminal different, respectively and the 2nd terminal different, respectively, and having the phase of transmitting reservation ticket information to the 2nd terminal also has the 1st desirable terminal.

[0010] As for the common key generation phase of a service provision phase, according to other operation gestalten of the approach of this invention, what (S46, S47) the common key KCS is generated also for based on the hash value computed from reservation ticket information is desirable.

[0011] According to other operation gestalten of the approach of this invention, the common key generation phase of a service provision phase The phase where a terminal generates the 3rd random number (R) itself (S42), and transmits this 3rd random number (R) and a reservation ticket information identifier (t-ID) to a server (S43), The phase where a terminal generates a common key based on a hash value, and the 3rd random number (R) and a reservation ticket information identifier (t-ID) (S47), It is also desirable that a server has the phase (S46) which generates a common key based on a hash value, and the 3rd random number (R) and a reservation ticket information identifier (t-ID).

[0012] According to other operation gestalten of the approach of this invention, the service provision authentication phase of a service provision phase The phase where a server transmits the 3rd random number (R) enciphered using the common key to a terminal (S48), The phase where a terminal decrypts the 3rd enciphered random number (R), compares this 3rd decrypted random number (R) with the 3rd random number (R) generated itself, and attests a server (S49), The phase of transmitting the reservation ticket information enciphered to the attested server using the common key to a server (S4A), It is also desirable to have the phase (S4B) which a server decrypts the enciphered reservation ticket information, compares this decrypted reservation ticket information with the reservation ticket information which the server published, and attests reservation ticket information.

[0013] according to other operation gestalten of the approach of this invention -- a service provision phase -- a service information transmitting phase (S4D) -- then, having the phase (S4G) of canceling reservation ticket information, and the phase (S4F) where a server cancels reservation ticket information also has a still more desirable terminal.

[0014] The phase where a terminal transmits a terminal side identifier (IDA) to a server according to other operation gestalten of the approach of this invention, It has further the terminal registration phase (S30) which consists of a phase where a server transmits the terminal side identifier (IDA) which received, and the key (MA) based on the private key (P) of the server concerned to a terminal. The service

reservation authentication phase of a service reservation phase The phase where a terminal generates the 1st random number (R) itself (S31), and transmits this 1st random number (R) and a terminal side identifier (IDA) to a server (S32), The phase where a terminal generates the prior common key MAS based on a key (MA), a terminal side identifier (IDA), and the 1st random number (R) (S34), The phase where a server generates the prior common key MAS using a function (fMA) based on a terminal side identifier (IDA) and the key (MA) based on the private key (P) of the server concerned and a terminal side identifier (IDA), and the 1st random number (R) (S33), The phase which a server generates the 2nd random number (R') itself (S35), enciphers the 1st random number (R) and this 2nd random number (R') with the prior common key MAS, and transmits to a terminal (S36), The phase where a server generates the common key KAS based on a terminal side identifier (IDA) and the 2nd random number (R') (S37), A terminal decrypts the 1st random number (R) and 2nd random number (R') using the prior common key MAS. The phase which attests the 1st server and generates the common key KAS based on a terminal side identifier (IDA) and the 2nd decrypted random number (R') when this 1st decrypted random number (R) is in agreement (S38), The phase which a terminal enciphers the 2nd random number (R') and user certificate using the common key KAS, and transmits to a server (S39), It is also desirable for a server to decrypt the 2nd random number (R') and reservation ticket information using the common key KAS, and to have the phase (S3A) which attests a terminal when this 2nd decrypted random number (R') is in agreement.

[0015] According to other operation gestalten of the approach of this invention, a server gives the signature of a server to reservation ticket information about the reservation ticket transmitting phase of a service reservation phase, and, as for a terminal, it is also desirable to give the signature based on a terminal side identifier to the received reservation ticket information.

[0016] A service reservation authentication means by which a terminal attests a server about a service reservation means according to the service reservation by the side of the terminal of this invention, and the distribution program (S38), A means (S3E) to receive reservation ticket information from this server, and a common key generation means to generate the common key KCS about a service provision phase based on reservation ticket information (S47), Operate a computer as a service provision authentication means (S49) to attest a server using this common key KCS, and according to the service reservation by the side of the server of this invention, and the distribution program a service reservation authentication means (S3A) by which a server attests a terminal about a service reservation means, and reservation ticket information -- a terminal -- transmitting (S3E) -- A reservation ticket transmitting means to memorize this reservation ticket information, and a common key generation means to generate the common key KCS about a service provision phase based on reservation ticket information (S46), A computer makes it function as

a service provision authentication means (S4B) to attest reservation ticket information using this common key KCS, and a service information transmitting means (S4D) to transmit service information to a terminal.
[0017] According to other operation gestalten of this invention, it is the record medium which recorded the above-mentioned program.
[0018]
[Embodiment of the Invention] The example of an outline of the operation gestalt of this invention is explained first. For example, a user reserves multimedia contents, such as a movie, at a house, and a case so that it may say that contents are downloaded from a mounted terminal is assumed at the point which went out by passenger car. In case a user reserves service, it attests by performing the check of the justification of the certificate which a user submits, the check of a user's service use authority, etc. After authentication, a service reception server is sent to a user at insurance while it publishes the reservation ticket used as the certification of having been attested correctly and service having been reserved correctly and holds it in person. A user copies the ticket to a personal digital assistant, and carries around at the time of going out. The reservation ticket which remained on the server on the other hand is sent on a management server, and it is kept by insurance until a user uses service. In case a user uses service at a going-out place, it verifies whether the reservation ticket sent from a management server and the reservation ticket sent from a personal digital assistant are in agreement on a service provision server, and considers as the simple authentication used as instead of [of the usual user authentication].
[0019] Below, the operation gestalt of this invention is explained to a detail using a drawing.
[0020] Drawing 3 is the sequence diagram of the service reservation phase by this invention.
[0021] As a premise, a user's terminal 14 performs one terminal registration (S30) to the service reception server 12. A terminal 14 transmits a terminal side identifier (IDA) to a server 12, and this transmits the terminal side identifier (IDA) which the server 12 received, and the key (MA=g (P|IDA)) based on the private key (P) of the server 12 concerned to a terminal 14. g() is a predetermined algorithm.
[0022] First, the service reservation authentication phase (S31-S3B) which attests a server 12 and a terminal 14 mutually is performed. A terminal 14 generates the 1st random number (R) itself (S31), and transmits this 1st random number (R) and a terminal side identifier (IDA) to a server 12 (S32). Next, a terminal 14 generates the prior common key MAS based on a key (MA), a terminal side identifier (IDA), and the 1st random number (R) (S34). Next, a server 12 generates the prior common key MAS using a function (fMA) based on a terminal side identifier (IDA) and the key (MA) based on the private key (P) of the server 12 concerned and a terminal side identifier (IDA), and the 1st random number (R) (S33). Next, a server 12 generates the 2nd

random number (R') itself (S35), enciphers the 1st random number (R) and this 2nd random number (R') with the prior common key MAS, and transmits to a terminal 14 (S36). Next, a server 12 generates the common key KAS based on a terminal side identifier (IDA) and the 2nd random number (R') (S37). Next, a terminal 14 decrypts the 1st random number (R) and 2nd random number (R') using the prior common key MAS, when this 1st decrypted random number (R) is in agreement, the 1st server 12 is attested and the common key KAS is generated based on a terminal side identifier (IDA) and the 2nd decrypted random number (R') (S38). Next, a terminal 14 enciphers the 2nd random number (R') and user certificate using the common key KAS, and transmits to a server 12 (S39). Next, a server 12 decrypts the 2nd random number (R') and reservation ticket information using the common key KAS, and a terminal 14 is attested when this 2nd decrypted random number (R') is in agreement (S3A).

[0023] Next, a reservation ticket transmitting phase is performed. A server 12 checks a certificate and transmits the completion of authentication, and reservation information to a terminal 14 (S3D). Next, a terminal 14 checks reservation information and requires the reservation (S3C). Next, a server 12 publishes a reservation ticket (S3D). The signature of the server 12 which shows the purport which the server 12 published is given to this reservation ticket. And a server 12 transmits reservation ticket information to a terminal 14 (S3E). A server 12 memorizes reservation ticket information then. The terminal 14 which received reservation ticket information gives the signature based on a terminal side identifier further to the reservation ticket information. A terminal 14 transmits this reservation ticket to a server 12 further. By this, the signature of the published server 12 and the signature of the terminal 14 which required issue will be given to the reservation ticket information which a server 12 and a terminal 14 hold.

[0024] According to this invention, it is premised on a reservation ticket moving among two or more terminals. In the usual general commercial transaction, it is because it does not say that those who purchased the reservation ticket surely receive offer of the service and the reservation ticket is what carries out **** circulation at other persons.

[0025] A user can memorize reservation ticket information to an IC card etc., and can also move to a mounted terminal. The reservation ticket information held by the service reception server 12 is transmitted to the management server 10. In the management server 10, reservation ticket information is kept until there is a user's access request. When a user accesses to the service provision server 11 through a terminal, the management server 10 transmits reservation ticket information to the service provision server 11 concerned.

[0026] Drawing 4 is the sequence diagram of a service provision phase. First, both a server 11 and the terminal 13 explain the common key generation phase (S41-S47) which generates the common key KCS based on reservation ticket information.

[0027] First, a server 11 transmits "Hello" which stimulates access to a terminal 13

(S41). On the other hand, a terminal 13 generates the 3rd random number (R) itself (S42), and transmits this 3rd random number (R) and a reservation ticket information identifier (t-ID) to a server 11 (S43). If a server 11 checks a reservation ticket information identifier (S44) and does not have the reservation ticket information are in agreement, at this time, an error will be transmitted to a terminal 13 (S45). When the reservation ticket information are in agreement exists, a terminal 13 generates the common key KCS based on the hash value computed from reservation ticket information, and the 3rd random number (R) and a reservation ticket information identifier (t-ID) (S47). Next, a server 11 generates the common key KCS based on the hash value computed from reservation ticket information, and the 3rd random number (R) and a reservation ticket information identifier (t-ID) (S46).

[0028] Next, the service provision authentication phase (S48-S4B) which attests a server and reservation ticket information using the common key KCS is performed. A server 11 transmits the 3rd random number (R) enciphered using the common key to a terminal 13 (S48). Next, a terminal 13 decrypts the 3rd enciphered random number (R), compares this 3rd decrypted random number (R) with the 3rd random number (R) generated itself, and attests a server 11 (S49). Next, the reservation ticket information enciphered to the attested server 11 using the common key is transmitted (S4A). Next, 11 and the enciphered reservation ticket information are decrypted, and a server compares this decrypted reservation ticket information with the reservation ticket information which the server 11 published, and attests reservation ticket information (S4B).

[0029] Next, a server 11 notifies download authorization to a terminal 13 (S4C). And service information transmission (S4D) which transmits service information to a terminal 13 is performed. It can come, and is alike, then a terminal 13 cancels reservation ticket information further (S4G), and a server 11 cancels reservation ticket information (S4F). At this time, a server 11 signs ticket used to reservation ticket information further.

[0030] According to the above-mentioned, although service reservation and the offer approach were explained, it can be easily hit on an idea of being realizable for a terminal and server side with the program of a computer. Therefore, according to this invention, it is applied also to the record medium which recorded the program which realizes the sequence between the terminals and servers based on the above-mentioned approach, and its program.

[0031] According to this contractor, various modification of the technical thought of this invention and the range of a standpoint, correction, and an abbreviation can carry out easily according to the various operation gestalten of this invention mentioned above. The above-mentioned explanation is an example to the last, and it is not going to restrain it at all. This invention is restrained by only what is limited as a claim and its equal object.

[0032]

[Effect of the Invention] As mentioned above, since a common key can be generated and used based on reservation ticket information according to this invention as explained to the detail, it is not necessary to adopt a public key system, and a dumb terminal with a comparatively small throughput can also realize authentication processing easily. This becomes possible [verifying justification almost comparable as the usual authentication processing]. Therefore, the time amount which authentication of service utilization time takes can be shortened, and it is effective in raising the convenience of service use.

[0033] This invention can secure the safety against the above thing while making applicability expand to an application which reserves and offers the service with which a personal digital assistant or a mounted terminal is provided.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1] It is the system configuration Fig. made into the object of this invention.

[Drawing 2] It is the sequence diagram of the conventional authentication approach.

[Drawing 3] It is the sequence diagram of the service reservation phase of this invention.

[Drawing 4] It is the sequence diagram of the service provision phase of this invention.

[Description of Notations]

10 Management Server

11 Service Provision Server

12 Service Reception Server

13 Personal Digital Assistant

14 User's Terminal

---

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号
特開2003－132253
（P2003－132253A）
(43)公開日　平成15年５月９日(2003.5.9)

(51)Int.Cl.[7]	識別記号	Ｆ Ｉ		テーマコード（参考）
Ｇ０６Ｆ　17/60	３２２	Ｇ０６Ｆ　17/60	３２２	５Ｊ１０４
	５１２		５１２	
	ＺＥＣ		ＺＥＣ	
Ｈ０４Ｌ　9/08		Ｈ０４Ｌ　9/00	６７５Ａ	
9/32			６０１Ｅ	

審査請求　未請求　請求項の数11　ＯＬ　（全 ９ 頁）

(21)出願番号　特願2001－323624(P2001－323624)

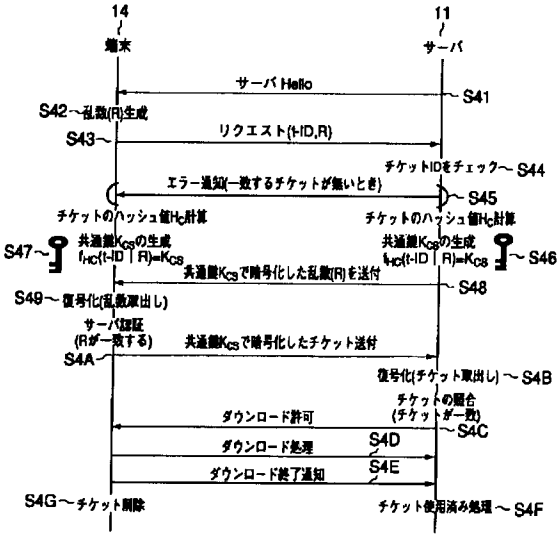
(22)出願日　平成13年10月22日(2001.10.22)

(71)出願人　000208891
ＫＤＤＩ株式会社
東京都新宿区西新宿二丁目３番２号
(71)出願人　301022471
独立行政法人通信総合研究所
東京都小金井市貫井北町４－２－１
(72)発明者　清本　晋作
埼玉県上福岡市大原二丁目１番15号　株式会社ケイディーディーアイ研究所内
(74)代理人　100074930
弁理士　山本　恵一

最終頁に続く

(54)【発明の名称】　チケットを用いて相互に認証するサービス予約及び提供方法、そのプログラム並びに該プログラムを記録した記録媒体

(57)【要約】
【課題】　電子商取引におけるサービスの予約段階及び提供段階のそれぞれについて、公開鍵暗号方式を用いることなく、処理能力の低い端末でも十分な認証能力を有することができる相互認証処理の方法、プログラム及び該プログラムを記録した記録媒体を提供する。
【解決手段】　サービス予約段階として、相互に認証し（Ｓ３１～Ｓ３Ｂ）、該サーバが予約チケット情報を端末へ送信する（Ｓ３Ｅ）と共に、該予約チケット情報を記憶し、サービス提供段階として、サーバと端末との両方が予約チケット情報に基づいて共通鍵ＫＣＳを生成し（Ｓ４１～Ｓ４７）、該共通鍵ＫＣＳを用いてサーバと予約チケット情報とを認証し（Ｓ４８～Ｓ４Ｂ）、サーバがサービス情報を端末へ送信する（Ｓ４Ｄ）。



【特許請求の範囲】

【請求項１】　サービス予約段階として、サーバと端末とを相互に認証するサービス予約認証段階（Ｓ３１～Ｓ３Ｂ）と、該サーバが、予約チケット情報を前記端末へ送信する（Ｓ３Ｅ）と共に、該予約チケット情報を記憶する予約チケット送信段階とを有し、

サービス提供段階として、サーバと端末との両方が、前記予約チケット情報に基づいて共通鍵ＫＣＳを生成する共通鍵生成段階（Ｓ４１～Ｓ４７）と、該共通鍵ＫＣＳを用いて前記サーバと前記予約チケット情報とを認証するサービス提供認証段階（Ｓ４８～Ｓ４Ｂ）と、前記サーバが前記サービス情報を前記端末へ送信するサービス情報送信段階（Ｓ４Ｄ）とを有することを特徴とするチケットを用いて相互に認証するサービス予約及び提供方法。

【請求項２】　前記サービス予約段階の前記サーバと、前記サービス提供段階の前記サーバとは、それぞれ異なる第１のサーバと第２のサーバとであり、前記第１のサーバが前記第２のサーバへ前記予約チケット情報を送信する段階を有することを特徴とする請求項１に記載の方法。

【請求項３】　前記サービス予約段階の前記端末と、前記サービス提供段階の前記端末とは、それぞれ異なる第１の端末と第２の端末とであり、前記第１の端末が前記第２の端末へ前記予約チケット情報を送信する段階を有することを特徴とする請求項１又は２に記載の方法。

【請求項４】　前記サービス提供段階の前記共通鍵生成段階は、前記予約チケット情報から算出したハッシュ値に基づいて前記共通鍵ＫＣＳを生成する（Ｓ４６、Ｓ４７）ことを特徴とする請求項１から３のいずれか１項に記載の方法。

【請求項５】　前記サービス提供段階の前記共通鍵生成段階は、

前記端末が、第３の乱数（Ｒ）を自ら生成し（Ｓ４２）、該第３の乱数（Ｒ）と前記予約チケット情報識別子（ｔ－ＩＤ）とを前記サーバへ送信する段階（Ｓ４３）と、

前記端末が、前記ハッシュ値と、前記第３の乱数（Ｒ）と前記予約チケット情報識別子（ｔ－ＩＤ）とに基づいて前記共通鍵を生成する段階（Ｓ４７）と、

前記サーバが、前記ハッシュ値と、前記第３の乱数（Ｒ）と前記予約チケット情報識別子（ｔ－ＩＤ）とに基づいて前記共通鍵を生成する段階（Ｓ４６）とを有することを特徴とする請求項４に記載の方法。

【請求項６】　前記サービス提供段階の前記サービス提供認証段階は、前記サーバが、前記共通鍵を用いて暗号化した前記第３の乱数（Ｒ）を前記端末へ送信する段階（Ｓ４８）と、

前記端末が、暗号化された前記第３の乱数（Ｒ）を復号化し、復号化された該第３の乱数（Ｒ）と自ら生成した前記第３の乱数（Ｒ）とを比較して前記サーバを認証する段階（Ｓ４９）と、認証された前記サーバへ前記共通鍵を用いて暗号化された前記予約チケット情報を前記サーバへ送信する段階（Ｓ４Ａ）と、

前記サーバが、暗号化された前記予約チケット情報を復号化し、復号化された該予約チケット情報と前記サーバが発行した前記予約チケット情報とを比較して前記予約チケット情報を認証する段階（Ｓ４Ｂ）とを有することを特徴とする請求項５に記載の方法。

【請求項７】　前記サービス提供段階は、前記サービス情報送信段階（Ｓ４Ｄ）に続いて、更に、

前記端末が、前記予約チケット情報を破棄する段階（Ｓ４Ｇ）と、

前記サーバが、前記予約チケット情報を破棄する段階（Ｓ４Ｆ）とを有することを特徴とする請求項１から６のいずれか１項に記載の方法。

【請求項８】　前記端末が、端末側識別子（ＩＤ$_A$）を前記サーバへ送信する段階と、前記サーバが、受信した前記端末側識別子（ＩＤ$_A$）及び当該サーバの秘密鍵（Ｐ）に基づく鍵（Ｍ$_A$）を前記端末へ送信する段階とからなる端末登録段階（Ｓ３０）を更に有し、

前記サービス予約段階の前記サービス予約認証段階は、

前記端末が、第１の乱数（Ｒ）を自ら生成し（Ｓ３１）、該第１の乱数（Ｒ）と端末側識別子（ＩＤ$_A$）とを前記サーバへ送信する段階（Ｓ３２）と、

前記端末が、前記鍵（Ｍ$_A$）と前記端末側識別子（ＩＤ$_A$）と前記第１の乱数（Ｒ）とに基づいて事前共通鍵ＭＡＳを生成する段階（Ｓ３４）と、

前記サーバが、前記端末側識別子（ＩＤ$_A$）及び当該サーバの秘密鍵（Ｐ）に基づく鍵（Ｍ$_A$）と前記端末側識別子（ＩＤ$_A$）と前記第１の乱数（Ｒ）とに基づいて前記関数（ｆ$_{MA}$）を用いて事前共通鍵ＭＡＳを生成する段階（Ｓ３３）と、

前記サーバが、第２の乱数（Ｒ′）を自ら生成し（Ｓ３５）、前記第１の乱数（Ｒ）と該第２の乱数（Ｒ′）とを前記事前共通鍵ＭＡＳで暗号化して前記端末へ送信する段階（Ｓ３６）と、

前記サーバが、前記端末側識別子（ＩＤ$_A$）と前記第２の乱数（Ｒ′）とに基づいて共通鍵ＫＡＳを生成する段階（Ｓ３７）と、

前記端末が、前記事前共通鍵ＭＡＳを用いて前記第１の乱数（Ｒ）と前記第２の乱数（Ｒ′）とを復号化し、復号化された該第１の乱数（Ｒ）が一致することにより前記第１のサーバを認証し、前記端末側識別子（ＩＤ$_A$）と復号化された前記第２の乱数（Ｒ′）とに基づいて共通鍵ＫＡＳを生成する段階（Ｓ３８）と、

前記端末が、前記共通鍵ＫＡＳを用いて前記第２の乱数（Ｒ′）と利用者証明書とを暗号化して前記サーバへ送信する段階（Ｓ３９）と、

前記サーバが、前記共通鍵ＫＡＳを用いて前記第２の乱

数（R′）と前記予約チケット情報とを復号化し、復号化された該第２の乱数（R′）が一致することにより前記端末を認証する段階（Ｓ３Ａ）とを有することを特徴とする請求項１から７のいずれか１項に記載の方法。
【請求項９】　前記サーバは、前記サービス予約段階の予約チケット送信段階について、前記予約チケット情報に前記サーバの署名を付与し、
前記端末は、受信した前記予約チケット情報に前記端末側識別子に基づく署名を付与することを特徴とする請求項１から８のいずれか１項に記載の方法。
【請求項１０】　端末が、サービス予約手段について、サーバを認証するサービス予約認証手段（Ｓ３８）と、該サーバから予約チケット情報を受信する手段（Ｓ３Ｅ）と、
サービス提供段階について、前記予約チケット情報に基づいて共通鍵ＫＣＳを生成する共通鍵生成手段（Ｓ４７）と、該共通鍵ＫＣＳを用いて前記サーバを認証するサービス提供認証手段（Ｓ４９）としてコンピュータを機能させることを特徴とする端末側のサービス予約及び提供プログラムと、
サーバが、サービス予約手段について、端末を認証するサービス予約認証手段（Ｓ３Ａ）と、予約チケット情報を前記端末へ送信する（Ｓ３Ｅ）と共に、該予約チケット情報を記憶する予約チケット送信手段とサービス提供段階について、前記予約チケット情報に基づいて共通鍵ＫＣＳを生成する共通鍵生成手段（Ｓ４６）と、該共通鍵ＫＣＳを用いて前記予約チケット情報を認証するサービス提供認証手段（Ｓ４Ｂ）と、前記サービス情報を前記端末へ送信するサービス情報送信手段（Ｓ４Ｄ）としてコンピュータを機能させることを特徴とするサーバ側のサービス予約及び提供プログラム。
【請求項１１】　請求項１０に記載のプログラムを記録した記録媒体。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、電子商取引において、サービスの予約段階及び提供段階のそれぞれに生じる相互認証処理の方法、プログラム及び該プログラムを記録した記録媒体に関する。
【０００２】
【従来の技術】近年、通信技術の発達により、大容量のマルチメディアコンテンツを携帯する端末やＩＴＳ（高度交通システム）における車載端末などで、外出先でダウンロードし閲覧する技術が検討され始めている。こうしたサービスでは、利用者は、家庭の端末で何らかのサービス予約を行い、外出先にて携帯する端末で、予約したサービスを利用するという形態をとる。その際、利用者の成りすましなどの不正利用を防止するために、利用者を適切に認証する必要がある。従来は、個々の場面において、同様の認証処理が行われていた。特に、認証処理のために公開鍵暗号化方式を採用していた。
【０００３】図１は、本発明が対象とするシステム構成図である。図１によれば、サービスを予約するサービス受付サーバ１２と、サービスを提供するサービス提供サーバ１１と、それらを管理する管理サーバ１０とが表されている。これらは、インターネットを介して相互接続されていることが好ましい。また、利用者の端末１４は、サービス受付サーバ１２にアクセスし、一定の認証処理の後に、特定のサービスを予約することができる。また、予約した端末１４のみならず、他の携帯端末１３から、サービス提供サーバ１１へアクセスし、一定の認証処理の後に、特定のサービスの提供を受けることができる。
【０００４】図２は、従来の認証シーケンス図である。最初に、サーバＡは、サーバＢへリクエストを送信する（Ｓ２１）。そのリクエストによって、サーバＡの公開鍵$Ｐ_Ａ$と証明書とがサーバＢへ送信される。サーバＢは、証明書をチェックし、乱数（R）を生成する（Ｓ２２）。次に、サーバＢは、サーバＡの公開鍵$Ｐ_Ａ$で暗号化した乱数（R）とサーバＢの識別子（$ＩＤ_Ｂ$）と、サーバＢの公開鍵$Ｐ_Ｂ$と証明書とを送信する（Ｓ２３）。これらを受信したサーバＡは、証明書をチェックし（Ｓ２４）、暗号化された乱数（R）とサーバＢの識別子（$ＩＤ_Ｂ$）とを復号化する。更に、サーバＡは、乱数R′を生成し、サーバＢの公開鍵$Ｐ_Ｂ$で暗号化した乱数（R、R′）及びサーバＡの識別子（$ＩＤ_Ａ$）をサーバＢへ送信する（Ｓ２５）。これにより、サーバＢは、暗号化された乱数（R、R′）を復号化し、その乱数（R）が一致することによってサーバＡを認証する（Ｓ２６）。これにより、サーバA及びサーバＢは、それぞれ共通鍵$Ｋ_ＡＢ$を生成する（Ｓ２７、Ｓ２８）。次に、サーバＢは、共通鍵$Ｋ_ＡＢ$で暗号化した乱数（R′）をサーバＡへ送信する（Ｓ２９）。これにより、サーバＡは、暗号化された乱数（R′）を復号化し、その乱数（R′）が一致することによってサーバＢを認証する（Ｓ２Ａ、Ｓ２Ｂ）。
【０００５】
【発明が解決しようとする課題】しかし、利用者を認証するために常に公開鍵暗号化方式を用いることは、認証処理の負荷を大きくする。パーソナルコンピュータのような設置された端末機器等と異なり、比較的処理能力の低いＰＤＡのような携帯端末で行うには、この問題は顕著となり、その処理に非常に長い時間を要する。その結果、サービスの利便性は低下してしまうことになりかねない。
【０００６】そこで、本発明は、電子商取引におけるサービスの予約段階及び提供段階のそれぞれについて、公開鍵暗号方式を用いることなく、処理能力の低い端末でも十分な認証能力を有することができる相互認証処理の方法、プログラム及び該プログラムを記録した記録媒体

を提供することを目的とする。

【０００７】

【課題を解決するための手段】本発明のチケットを用いて相互に認証するサービス予約及び提供方法によれば、サービス予約段階として、サーバと端末とを相互に認証するサービス予約認証段階（Ｓ３１～Ｓ３Ｂ）と、該サーバが、予約チケット情報を端末へ送信する（Ｓ３Ｅ）と共に、該予約チケット情報を記憶する予約チケット送信段階とを有し、サービス提供段階として、サーバと端末との両方が、予約チケット情報に基づいて共通鍵ＫＣＳを生成する共通鍵生成段階（Ｓ４１～Ｓ４７）と、該共通鍵ＫＣＳを用いてサーバと予約チケット情報とを認証するサービス提供認証段階（Ｓ４８～Ｓ４Ｂ）と、サーバがサービス情報を端末へ送信するサービス情報送信段階（Ｓ４Ｄ）とを有する。即ち、本発明の特徴は、最初の認証の際に適切な認証を行った上で予約チケット情報の発行を行い、その後の認証処理については、予約チケット情報を用いて認証を行うことで、認証処理のための負荷を軽減することができる。

【０００８】本発明の方法の他の実施形態によれば、サービス予約段階のサーバと、サービス提供段階のサーバとは、それぞれ異なる第１のサーバと第２のサーバとであり、第１のサーバが第２のサーバへ予約チケット情報を送信する段階を有することも好ましい。

【０００９】本発明の方法の他の実施形態によれば、サービス予約段階の端末と、サービス提供段階の端末とは、それぞれ異なる第１の端末と第２の端末とであり、第１の端末が第２の端末へ予約チケット情報を送信する段階を有することも好ましい。

【００１０】本発明の方法の他の実施形態によれば、サービス提供段階の共通鍵生成段階は、予約チケット情報から算出したハッシュ値に基づいて共通鍵ＫＣＳを生成する（Ｓ４６、Ｓ４７）ことも好ましい。

【００１１】本発明の方法の他の実施形態によれば、サービス提供段階の共通鍵生成段階は、端末が、第３の乱数（Ｒ）を自ら生成し（Ｓ４２）、該第３の乱数（Ｒ）と予約チケット情報識別子（ｔ－ＩＤ）とをサーバへ送信する段階（Ｓ４３）と、端末が、ハッシュ値と、第３の乱数（Ｒ）と予約チケット情報識別子（ｔ－ＩＤ）とに基づいて共通鍵を生成する段階（Ｓ４７）と、サーバが、ハッシュ値と、第３の乱数（Ｒ）と予約チケット情報識別子（ｔ－ＩＤ）とに基づいて共通鍵を生成する段階（Ｓ４６）とを有することも好ましい。

【００１２】本発明の方法の他の実施形態によれば、サービス提供段階のサービス提供認証段階は、サーバが、共通鍵を用いて暗号化した第３の乱数（Ｒ）を端末へ送信する段階（Ｓ４８）と、端末が、暗号化された第３の乱数（Ｒ）を復号化し、復号化された該第３の乱数（Ｒ）と自ら生成した第３の乱数（Ｒ）とを比較してサーバを認証する段階（Ｓ４９）と、認証されたサーバへ共通鍵を用いて暗号化された予約チケット情報をサーバへ送信する段階（Ｓ４Ａ）と、サーバが、暗号化された予約チケット情報を復号化し、復号化された該予約チケット情報とサーバが発行した予約チケット情報とを比較して予約チケット情報を認証する段階（Ｓ４Ｂ）とを有することも好ましい。

【００１３】本発明の方法の他の実施形態によれば、サービス提供段階は、サービス情報送信段階（Ｓ４Ｄ）に続いて、更に、端末が、予約チケット情報を破棄する段階（Ｓ４Ｇ）と、サーバが、予約チケット情報を破棄する段階（Ｓ４Ｆ）とを有することも好ましい。

【００１４】本発明の方法の他の実施形態によれば、端末が、端末側識別子（ＩＤ$_A$）をサーバへ送信する段階と、サーバが、受信した端末側識別子（ＩＤ$_A$）及び当該サーバの秘密鍵（Ｐ）に基づく鍵（Ｍ$_A$）を端末へ送信する段階とからなる端末登録段階（Ｓ３０）を更に有し、サービス予約段階のサービス予約認証段階は、端末が、第１の乱数（Ｒ）を自ら生成し（Ｓ３１）、該第１の乱数（Ｒ）と端末側識別子（ＩＤ$_A$）とをサーバへ送信する段階（Ｓ３２）と、端末が、鍵（Ｍ$_A$）と端末側識別子（ＩＤ$_A$）と第１の乱数（Ｒ）とに基づいて事前共通鍵ＭＡＳを生成する段階（Ｓ３４）と、サーバが、端末側識別子（ＩＤ$_A$）及び当該サーバの秘密鍵（Ｐ）に基づく鍵（Ｍ$_A$）と端末側識別子（ＩＤ$_A$）と第１の乱数（Ｒ）とに基づいて関数（ｆ$_{MA}$）を用いて事前共通鍵ＭＡＳを生成する段階（Ｓ３３）と、サーバが、第２の乱数（Ｒ′）を自ら生成し（Ｓ３５）、第１の乱数（Ｒ）と該第２の乱数（Ｒ′）とを事前共通鍵ＭＡＳで暗号化して端末へ送信する段階（Ｓ３６）と、サーバが、端末側識別子（ＩＤ$_A$）と第２の乱数（Ｒ′）とに基づいて共通鍵ＫＡＳを生成する段階（Ｓ３７）と、端末が、事前共通鍵ＭＡＳを用いて第１の乱数（Ｒ）と第２の乱数（Ｒ′）とを復号化し、復号化された該第１の乱数（Ｒ）が一致することにより第１のサーバを認証し、端末側識別子（ＩＤ$_A$）と復号化された第２の乱数（Ｒ′）とに基づいて共通鍵ＫＡＳを生成する段階（Ｓ３８）と、端末が、共通鍵ＫＡＳを用いて第２の乱数（Ｒ′）と利用者証明書とを暗号化してサーバへ送信する段階（Ｓ３９）と、サーバが、共通鍵ＫＡＳを用いて第２の乱数（Ｒ′）と予約チケット情報とを復号化し、復号化された該第２の乱数（Ｒ′）が一致することにより端末を認証する段階（Ｓ３Ａ）とを有することも好ましい。

【００１５】本発明の方法の他の実施形態によれば、サーバは、サービス予約段階の予約チケット送信段階について、予約チケット情報にサーバの署名を付与し、端末は、受信した予約チケット情報に端末側識別子に基づく署名を付与することも好ましい。

【００１６】本発明の端末側のサービス予約及び提供プログラムによれば、端末が、サービス予約手段につい

て、サーバを認証するサービス予約認証手段（Ｓ３８）と、該サーバから予約チケット情報を受信する手段（Ｓ３Ｅ）と、サービス提供段階について、予約チケット情報に基づいて共通鍵ＫＣＳを生成する共通鍵生成手段（Ｓ４７）と、該共通鍵ＫＣＳを用いてサーバを認証するサービス提供認証手段（Ｓ４９）としてコンピュータを機能させ、本発明のサーバ側のサービス予約及び提供プログラムによれば、サーバが、サービス予約手段について、端末を認証するサービス予約認証手段（Ｓ３Ａ）と、予約チケット情報を端末へ送信する（Ｓ３Ｅ）と共に、該予約チケット情報を記憶する予約チケット送信手段と、サービス提供段階について、予約チケット情報に基づいて共通鍵ＫＣＳを生成する共通鍵生成手段（Ｓ４６）と、該共通鍵ＫＣＳを用いて予約チケット情報を認証するサービス提供認証手段（Ｓ４Ｂ）と、サービス情報を端末へ送信するサービス情報送信手段（Ｓ４Ｄ）としてコンピュータが機能させるものである。

【００１７】本発明の他の実施形態によれば、前述のプログラムを記録した記録媒体である。

【００１８】

【発明の実施の形態】本発明の実施形態の概要例を最初に説明する。例えば、利用者が自宅にて、映画などのマルチメディアコンテンツの予約を行い、乗用車で外出した先で、車載端末よりコンテンツのダウンロードを行うというような場合を想定する。利用者が、サービスの予約をする際には、利用者が提出する証明書の正当性の確認、利用者のサービス利用権限の確認等を行い、認証を行う。認証後、サービス受付サーバは、正しく認証されたことと、サービスが正しく予約されたことの証明となる予約チケットを発行し、自身で保持すると共に、利用者に安全に送付する。利用者は、そのチケットを携帯端末へと写し、外出時には持ち歩く。一方サーバ上に残った予約チケットは、管理サーバ上に送られ、利用者がサービスを利用するときまで安全に保管される。利用者が外出先でサービスを利用する際には、サービス提供サーバ上で、管理サーバから送られてくる予約チケットと、携帯端末から送られてくる予約チケットが一致するか検証を行い、通常の利用者認証の代わりとなる簡易認証とする。

【００１９】以下では、図面を用いて、本発明の実施形態を詳細に説明する。

【００２０】図３は、本発明によるサービス予約段階のシーケンス図である。

【００２１】前提として、利用者の端末１４は、サービス受付サーバ１２に対して、１回の端末登録（Ｓ３０）を行う。これは、端末１４が、端末側識別子（ID_A）をサーバ１２へ送信し、サーバ１２が、受信した端末側識別子（ID_A）及び当該サーバ１２の秘密鍵（Ｐ）に基づく鍵（$M_A = g(P \mid ID_A)$）を端末１４へ送信する。ｇ（）は、所定のアルゴリズムである。

【００２２】最初に、サーバ１２と端末１４とを相互に認証するサービス予約認証段階（Ｓ３１～Ｓ３Ｂ）が行われる。端末１４が、第１の乱数（Ｒ）を自ら生成し（Ｓ３１）、該第１の乱数（Ｒ）と端末側識別子（ID_A）とをサーバ１２へ送信する（Ｓ３２）。次に、端末１４が、鍵（M_A）と端末側識別子（ID_A）と第１の乱数（Ｒ）とに基づいて事前共通鍵M_{AS}を生成する（Ｓ３４）。次に、サーバ１２が、端末側識別子（ID_A）及び当該サーバ１２の秘密鍵（Ｐ）に基づく鍵（M_A）と端末側識別子（ID_A）と第１の乱数（Ｒ）とに基づいて関数（f_{MA}）を用いて事前共通鍵M_{AS}を生成する（Ｓ３３）。次に、サーバ１２が、第２の乱数（Ｒ′）を自ら生成し（Ｓ３５）、第１の乱数（Ｒ）と該第２の乱数（Ｒ′）とを事前共通鍵M_{AS}で暗号化して端末１４へ送信する（Ｓ３６）。次に、サーバ１２が、端末側識別子（ID_A）と第２の乱数（Ｒ′）とに基づいて共通鍵K_{AS}を生成する（Ｓ３７）。次に、端末１４が、事前共通鍵M_{AS}を用いて第１の乱数（Ｒ）と第２の乱数（Ｒ′）とを復号化し、復号化された該第１の乱数（Ｒ）が一致することにより第１のサーバ１２を認証し、端末側識別子（ID_A）と復号化された第２の乱数（Ｒ′）とに基づいて共通鍵K_{AS}を生成する（Ｓ３８）。次に、端末１４が、共通鍵K_{AS}を用いて第２の乱数（Ｒ′）と利用者証明書とを暗号化してサーバ１２へ送信する（Ｓ３９）。次に、サーバ１２が、共通鍵K_{AS}を用いて第２の乱数（Ｒ′）と予約チケット情報とを復号化し、復号化された該第２の乱数（Ｒ′）が一致することにより端末１４を認証する（Ｓ３Ａ）。

【００２３】次に、予約チケット送信段階が行われる。サーバ１２が、証明書をチェックし、認証完了と予約情報とを端末１４へ送信する（Ｓ３Ｄ）。次に、端末１４は、予約情報をチェックし、その予約を要求する（Ｓ３Ｃ）。次に、サーバ１２が、予約チケットを発行する（Ｓ３Ｄ）。この予約チケットには、サーバ１２が発行した旨を示すサーバ１２の署名が付与される。そして、サーバ１２は、予約チケット情報を端末１４へ送信する（Ｓ３Ｅ）。そのとき、サーバ１２は、予約チケット情報を記憶する。予約チケット情報を受信した端末１４は、その予約チケット情報に端末側識別子に基づく署名を更に付与する。端末１４は、この予約チケットは、更に、サーバ１２へ送信する。これにより、サーバ１２及び端末１４が保持する予約チケット情報には、発行したサーバ１２の署名と、発行を要求した端末１４の署名とが付与されていることになる。

【００２４】本発明によれば、予約チケットが複数の端末間で移動することを前提としている。通常の一般的な商取引において、予約チケットを購入した者が必ずそのサービスの提供を受けるというものではなく、その予約チケットは他の者に転々流通するものだからである。

【００２５】利用者は、予約チケット情報をＩＣカード

等に記憶し、車載端末へと移すこともできる。サービス受付サーバ１２で保持された予約チケット情報は、管理サーバ１０へ送信される。管理サーバ１０では、予約チケット情報を利用者のアクセス要求があるまで保管する。利用者が端末を介してサービス提供サーバ１１へアクセスすることにより、管理サーバ１０が、当該サービス提供サーバ１１へ予約チケット情報を送信する。

【００２６】図４は、サービス提供段階のシーケンス図である。最初に、サーバ１１と端末１３との両方が、予約チケット情報に基づいて共通鍵ＫＣＳを生成する共通鍵生成段階（Ｓ４１～Ｓ４７）について説明する。

【００２７】最初に、サーバ１１は、端末１３へアクセスを促す「Ｈｅｌｌｏ」を送信する（Ｓ４１）。これに対して、端末１３が、第３の乱数（Ｒ）を自ら生成し（Ｓ４２）、該第３の乱数（Ｒ）と予約チケット情報識別子（ｔ－ＩＤ）とをサーバ１１へ送信する（Ｓ４３）。このとき、サーバ１１は、予約チケット情報識別子をチェックし（Ｓ４４）、一致する予約チケット情報がなければ、エラーを端末１３へ送信する（Ｓ４５）。一致する予約チケット情報が存在する場合、端末１３が、予約チケット情報から算出したハッシュ値と、第３の乱数（Ｒ）と予約チケット情報識別子（ｔ－ＩＤ）とに基づいて共通鍵ＫＣＳを生成する（Ｓ４７）。次に、サーバ１１が、予約チケット情報から算出したハッシュ値と、第３の乱数（Ｒ）と予約チケット情報識別子（ｔ－ＩＤ）とに基づいて共通鍵ＫＣＳを生成する（Ｓ４６）。

【００２８】次に、共通鍵ＫＣＳを用いてサーバと予約チケット情報とを認証するサービス提供認証段階（Ｓ４８～Ｓ４Ｂ）を行う。サーバ１１が、共通鍵を用いて暗号化した第３の乱数（Ｒ）を端末１３へ送信する（Ｓ４８）。次に、端末１３が、暗号化された第３の乱数（Ｒ）を復号化し、復号化された該第３の乱数（Ｒ）と自ら生成した第３の乱数（Ｒ）とを比較してサーバ１１を認証する（Ｓ４９）。次に、認証されたサーバ１１へ共通鍵を用いて暗号化された予約チケット情報を送信する（Ｓ４Ａ）。次に、サーバが１１、暗号化された予約チケット情報を復号化し、復号化された該予約チケット情報とサーバ１１が発行した予約チケット情報とを比較して予約チケット情報を認証する（Ｓ４Ｂ）。

【００２９】次に、サーバ１１が、端末１３へダウンロード許可を通知する（Ｓ４Ｃ）。そして、サービス情報を端末１３へ送信するサービス情報送信（Ｓ４Ｄ）が行われる。これに続いて、更に、端末１３が、予約チケット情報を破棄し（Ｓ４Ｇ）、サーバ１１が、予約チケット情報を破棄する（Ｓ４Ｆ）。このとき、サーバ１１は、予約チケット情報に、チケット使用済みの署名を更に行う。

【００３０】前述によれば、サービス予約及び提供方法について説明したが、端末側及びサーバ側においてコンピュータのプログラムによって実現できることは、容易に想到できる。従って、本発明によれば、前述の方法に基づく端末とサーバとの間のシーケンスを実現するプログラム及びそのプログラムを記録した記録媒体にも適用される。

【００３１】前述した本発明の種々の実施形態によれば、本発明の技術思想及び見地の範囲の種々の変更、修正及び省略が、当業者によれば容易に行うことができる。前述の説明はあくまで例であって、何ら制約しようとするものではない。本発明は、特許請求の範囲及びその均等物として限定するものにのみ制約される。

【００３２】

【発明の効果】以上、詳細に説明したように、本発明によれば、予約チケット情報に基づいて共通鍵を生成し利用することができるので、公開鍵方式を採用する必要がなく、比較的処理能力の小さい簡易端末でも認証処理を容易に実現することができる。これは、通常の認証処理とほぼ同程度の正当性を検証することが可能となる。従って、サービス利用時の認証に要する時間を短縮することができ、サービス利用の利便性を向上させるという効果がある。

【００３３】以上のことから、本発明は、携帯端末又は車載端末に提供するサービスを予約及び提供するような用途に適用範囲を拡大させると共に、その安全性を保障することができる。

【図面の簡単な説明】

【図１】本発明の対象とするシステム構成図である。

【図２】従来の認証方法のシーケンス図である。

【図３】本発明のサービス予約段階のシーケンス図である。

【図４】本発明のサービス提供段階のシーケンス図である。

【符号の説明】

１０　管理サーバ

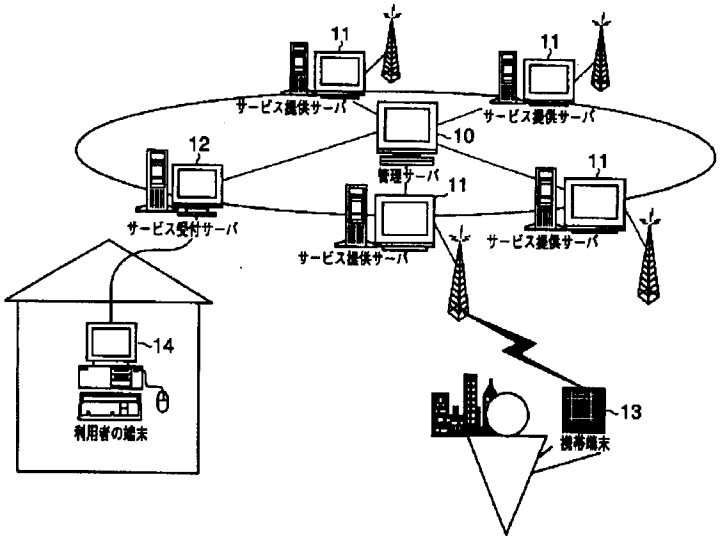
１１　サービス提供サーバ

１２　サービス受付サーバ

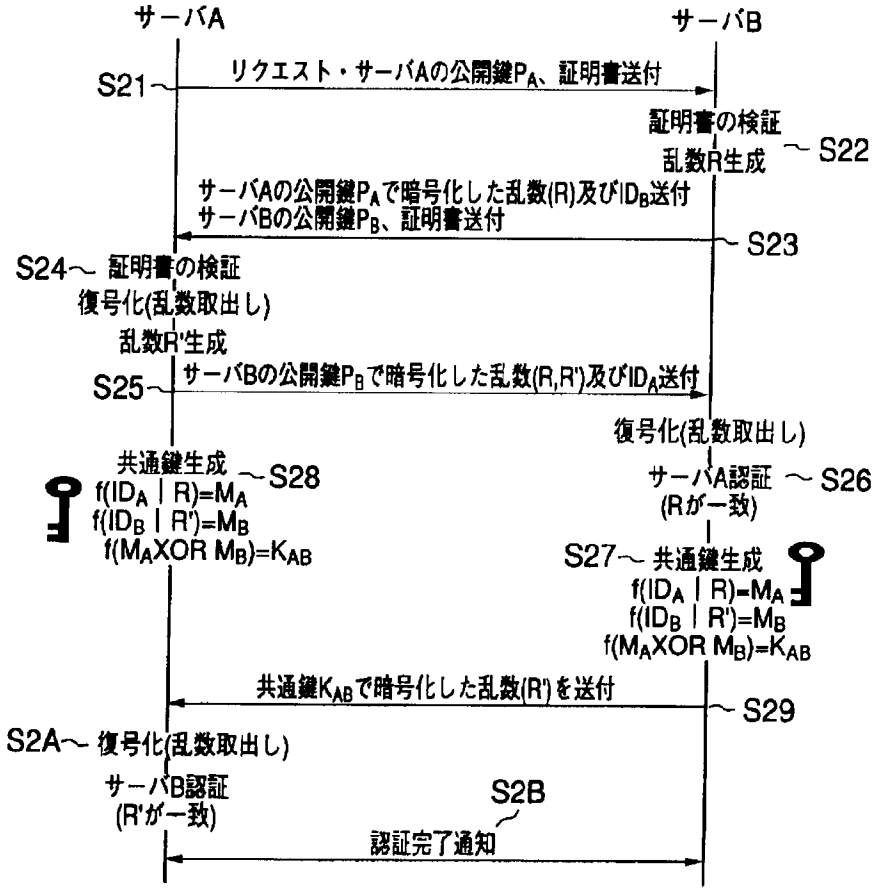
１３　携帯端末

１４　利用者の端末

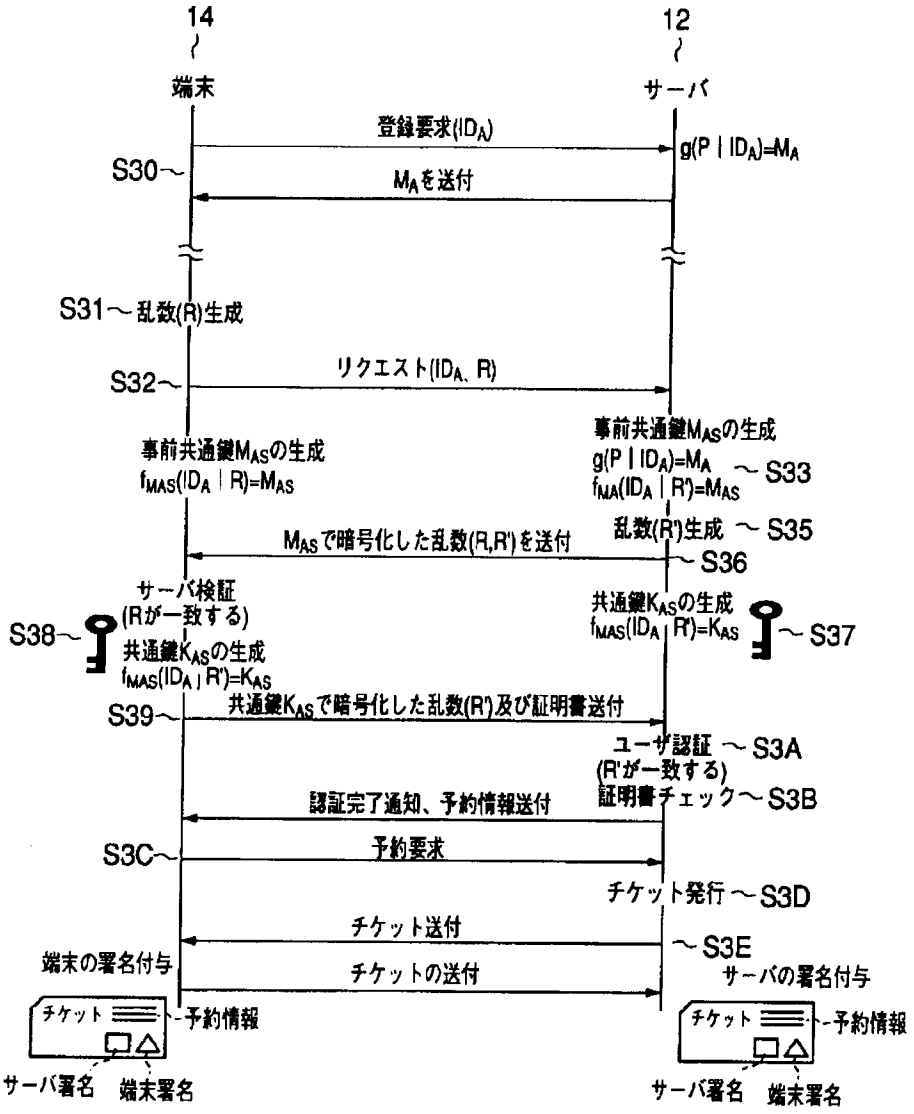
【図１】


11
サービス提供サーバ
11
サービス提供サーバ
10
管理サーバ
12
サービス受付サーバ
11
サービス提供サーバ
11
サービス提供サーバ
14
利用者の端末
13
携帯端末

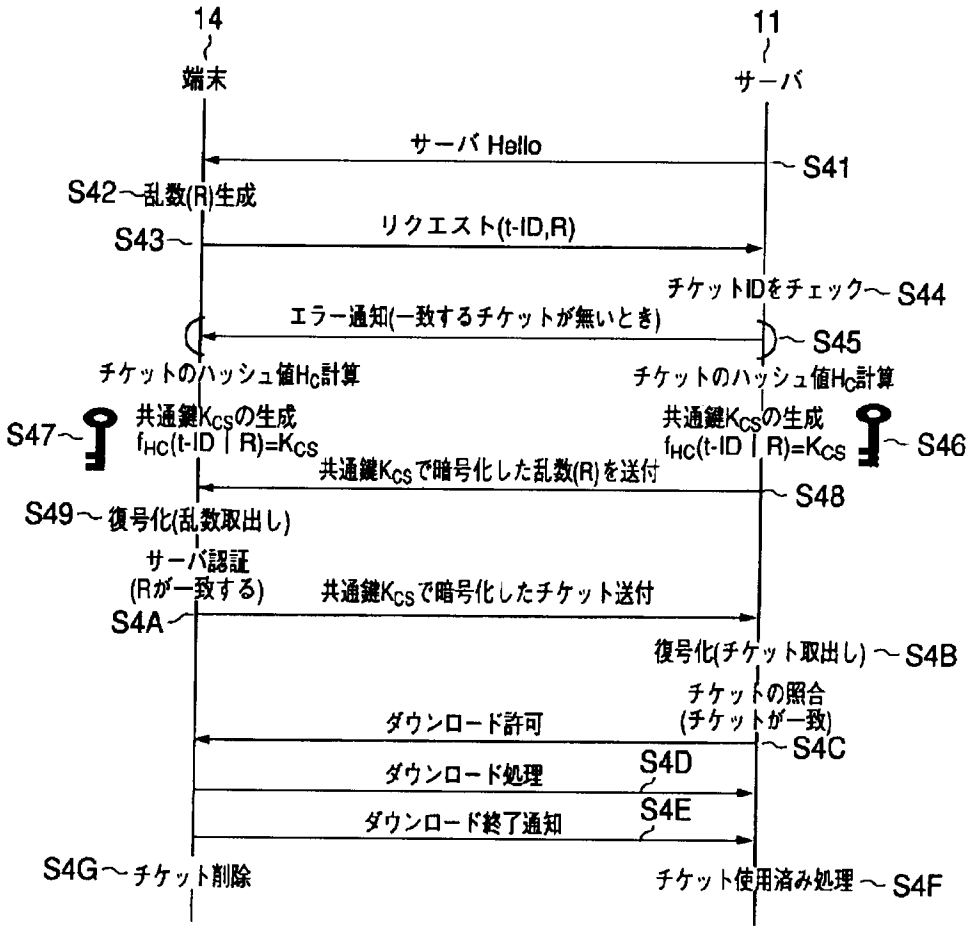
【図２】


サーバA
サーバB
S21
リクエスト・サーバAの公開鍵P_A、証明書送付
証明書の検証
乱数R生成
S22
サーバAの公開鍵P_Aで暗号化した乱数(R)及びID_B送付
サーバBの公開鍵P_B、証明書送付
S23
S24
証明書の検証
復号化(乱数取出し)
乱数R'生成
S25
サーバBの公開鍵P_Bで暗号化した乱数(R,R')及びID_A送付
復号化(乱数取出し)
共通鍵生成
S28
$f(ID_A \mid R)=M_A$
$f(ID_B \mid R')=M_B$
$f(M_A XOR M_B)=K_{AB}$
サーバA認証
S26
(Rが一致)
S27
共通鍵生成
$f(ID_A \mid R)=M_A$
$f(ID_B \mid R')=M_B$
$f(M_A XOR M_B)=K_{AB}$
共通鍵K_{AB}で暗号化した乱数(R')を送付
S29
S2A
復号化(乱数取出し)
サーバB認証
(R'が一致)
S2B
認証完了通知

【図３】


14
端末
12
サーバ
登録要求(IDA)
g(P | IDA)=MA
S30
MAを送付
S31
乱数(R)生成
S32
リクエスト(IDA、R)
事前共通鍵MASの生成
fMAS(IDA | R)=MAS
事前共通鍵MASの生成
g(P | IDA)=MA
fMA(IDA | R')=MAS
S33
乱数(R')生成
S35
MASで暗号化した乱数(R,R')を送付
S36
サーバ検証
(Rが一致する)
S38
共通鍵KASの生成
fMAS(IDA | R')=KAS
共通鍵KASの生成
fMAS(IDA | R')=KAS
S37
S39
共通鍵KASで暗号化した乱数(R')及び証明書送付
ユーザ認証
(R'が一致する)
証明書チェック
S3A
S3B
認証完了通知、予約情報送付
S3C
予約要求
チケット発行
S3D
チケット送付
S3E
端末の署名付与
チケットの送付
サーバの署名付与
チケット
予約情報
チケット
予約情報
サーバ署名
端末署名
サーバ署名
端末署名

【図４】



フロントページの続き

(72)発明者　田中　俊昭
埼玉県上福岡市大原二丁目１番15号　株式会社ケイディーディーアイ研究所内
(72)発明者　中尾　康二
埼玉県上福岡市大原二丁目１番15号　株式会社ケイディーディーアイ研究所内
(72)発明者　藤瀬　雅行
東京都小金井市貫井北町４－２－１　独立行政法人通信総合研究所内
(72)発明者　児島　史秀
東京都小金井市貫井北町４－２－１　独立行政法人通信総合研究所内
(72)発明者　佐藤　勝善
東京都小金井市貫井北町４－２－１　独立行政法人通信総合研究所内

Ｆターム(参考)　5J104 AA07 AA18 KA02 KA04 KA06 NA02 PA10